

10.11.2004

日本国特許庁  
JAPAN PATENT OFFICE

#2

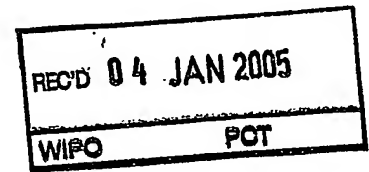
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年11月21日  
Date of Application:

出願番号 特願2003-392377  
Application Number:  
[ST. 10/C]: [JP2003-392377]

出願人 キヤノン株式会社  
Applicant(s):



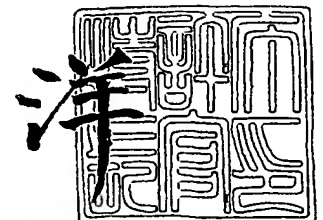
PRIORITY  
DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2004年12月17日

特許庁長官  
Commissioner,  
Japan Patent Office

BEST AVAILABLE COPY

小川



【書類名】 特許願  
【整理番号】 256838  
【提出日】 平成15年11月21日  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 12/14 320  
【発明者】  
    【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内  
    【氏名】 鈴木 勝也  
【特許出願人】  
    【識別番号】 000001007  
    【氏名又は名称】 キヤノン株式会社  
    【代表者】 御手洗 富士夫  
【代理人】  
    【識別番号】 100081880  
    【弁理士】  
    【氏名又は名称】 渡部 敏彦  
    【電話番号】 03(3580)8464  
【手数料の表示】  
    【予納台帳番号】 007065  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9703713

**【書類名】 特許請求の範囲****【請求項 1】**

非接触 IC に記録された機密データが機密エリアの外部で漏洩するのを防止するセキュリティシステムであって、

前記機密エリアに対する前記非接触 IC の持出し／持込み状況を検知する検知手段と、  
前記検知手段により、前記機密エリアからの前記非接触 IC の持出しが検知された場合に、当該非接触 IC に記録された機密データに対して所定の漏洩防止処理を施す漏洩防止手段と、

を有することを特徴とするセキュリティシステム。

**【請求項 2】**

前記漏洩防止手段は、前記非接触 IC に記録された機密データを所定の装置に退避した後に、該非接触 IC に記録された退避に係る機密データを消去することを特徴とする請求項 1 に記載のセキュリティシステム。

**【請求項 3】**

前記漏洩防止手段は、前記非接触 IC が機密エリアの中に持込まれる場合に、前記サーバ装置に退避した機密データを該非接触 IC に書き戻す書戻手段を有することを特徴とする請求項 2 に記載のセキュリティシステム。

**【請求項 4】**

前記漏洩防止手段は、前記非接触 IC に記録された機密データをアクセス不可状態にすることを特徴とする請求項 1 に記載のセキュリティシステム。

**【請求項 5】**

非接触 IC に記録された情報を非接触にてアクセスするリーダ／ライタを備えたゲート手段を含むセキュリティシステムであって、

前記リーダ／ライタは、前記ゲート手段によって形成されるセキュリティエリアの外に前記非接触 IC が持出される場合に、該非接触 IC に記録された機密データに対して前記リーダ／ライタを用いて所定の漏洩防止処理を施す制御手段を有することを特徴とするセキュリティシステム。

**【請求項 6】**

前記制御手段は、前記非接触 IC に記録された機密データを読み取って所定の装置に退避した後に、該非接触 IC に記録された退避に係る機密データを消去することを特徴とする請求項 5 に記載のセキュリティシステム。

**【請求項 7】**

前記制御手段は、前記非接触 IC が前記セキュリティエリアの中に持込まれる場合に、前記所定の装置に退避した機密データを該非接触 IC に書き戻す書戻手段を有することを特徴とする請求項 6 に記載のセキュリティシステム。

**【請求項 8】**

前記制御手段は、前記非接触 IC に記録された機密データをアクセス不可状態にすることを特徴とする請求項 5 に記載のセキュリティシステム。

**【請求項 9】**

非接触 IC に記録された機密データが機密エリアの外部で漏洩するのを防止するセキュリティシステムの制御方法であって、

前記機密エリアに対する前記非接触 IC の持出し／持込み状況を検知する検知工程と、  
前記検知工程により、前記機密エリアからの前記非接触 IC の持出しが検知された場合に、当該非接触 IC に記録された機密データに対して所定の漏洩防止処理を施す漏洩防止工程と、

を有することを特徴とするセキュリティシステムの制御方法。

**【請求項 10】**

非接触 IC に記録された情報を非接触にてアクセスするリーダ／ライタを備えたゲート手段を含むセキュリティシステムの制御方法であって、

前記リーダ／ライタは、前記ゲート手段によって形成されるセキュリティエリアの外に

前記非接触 I D が持出される場合に、該非接触 I C に記録された機密データに対して前記リーダ／ライタを用いて所定の漏洩防止処理を施す制御工程を有することを特徴とするセキュリティシステムの制御方法。

【請求項 11】

非接触 I C に記録された機密データが機密エリアの外部で漏洩するのを防止するセキュリティシステムにおける該非接触 I C 用のプログラムであって、

前記機密エリアに対する前記非接触 I C の持出し／持込み状況を検知する検知処理と、該検知処理により、前記機密エリアからの前記非接触 I C の持出しが検知された場合に、当該非接触 I C に記録された機密データに対する所定の漏洩防止処理とを行う内容を有することを特徴とするプログラム。

【請求項 12】

非接触 I C に記録された情報を非接触にてアクセスするリーダ／ライタを備えたゲート手段を含むセキュリティシステムにおける該リーダ／ライタ用のプログラムであって、

前記ゲート手段によって形成されるセキュリティエリアの外に前記非接触 I D が持出される場合に、該非接触 I C に記録された機密データに対して所定の漏洩防止処理を施す内容を有することを特徴とするプログラム。

【請求項 13】

非接触 I C に記録された情報を非接触にてアクセスするリーダ／ライタを備えたゲート手段を有するセキュリティシステムにおける該非接触 I C 用のプログラムであって、

前記ゲート手段によって形成されるセキュリティエリアの外に前記非接触 I D が持出される場合に、前記リーダ／ライタからの指示に応じて、該非接触 I C に記録された機密データに対して所定の漏洩防止処理を施す内容を有することを特徴とするプログラム。

**【書類名】 明細書****【発明の名称】 セキュリティシステム****【技術分野】****【0001】**

本発明は、RFID (Radio Frequency Identification) タグのような非接触 IC に格納された機密データを保護する技術に関する。

**【背景技術】****【0002】**

従来、磁気カード等の可搬性のある記憶媒体等を用いて入退出管理を行うセキュリティシステムが実現されている (例えば、特許文献 1 参照)。

**【特許文献 1】** 特開平 11-303478 号公報

**【発明の開示】****【発明が解決しようとする課題】****【0003】**

ところで、RFID タグのような非接触 IC の利用形態として、例えば、非接触 IC 内のメモリに MFP (複合機) に対するジョブ情報を格納し、このジョブ情報を非接触で MFP にダウンロードして実行させることが考えられる。

**【0004】**

このような利用形態において、非接触 IC のメモリに社外秘、或いは部門外秘等の機密データ (ジョブ情報、コマンドを含む) を格納した状態で、この非接触 IC を社外、或いは部門外等に持ち出した際に紛失してしまったような場合に、非接触 IC 内のメモリに格納された機密データが第 3 者により読み出されてしまい、機密状態を維持できなくなって、機密データのセキュリティが低下する可能性がある。

**【0005】**

そこで、本発明は、非接触 IC に格納された機密データが所定エリア外で第 3 者に漏洩するのを防止し得るセキュリティシステム、その制御方法、及びプログラムを提供することを目的とする。

**【課題を解決するための手段】****【0006】**

上記目的を達成するため、本発明は、非接触 IC に記録された機密データが機密エリアの外部で漏洩するのを防止するセキュリティシステムであって、前記機密エリアに対する前記非接触 IC の持出し／持込み状況を検知する検知手段と、前記検知手段により、前記機密エリアからの前記非接触 IC の持出しが検知された場合に、当該非接触 IC に記録された機密データに対して所定の漏洩防止処理を施す漏洩防止手段とを有している。

**【発明の効果】****【0007】**

本発明によれば、非接触 IC に格納された機密データが所定エリア外で第 3 者に漏洩するのを防止し得るセキュリティシステム、その制御方法、及びプログラムを提供することが可能となり、第 3 者による機密データの悪用を回避することが可能となる。

**【発明を実施するための最良の形態】****【0008】**

以下、本発明を実施するための最良の形態を、図面に基づいて詳細に説明する。

**【0009】**

図 1 は、本発明に係るセキュリティシステムのシステム構成図である。本システムにおいては、門、ドア等の物理的な複数のゲートや物理的な壁 (不図示) 等によって外界から区分されたセキュリティエリア (機密エリアとも言う) 100 を想定しており、このセキュリティエリア 100 内には、セキュリティサーバ 103、MFP (複合機) 105、文書サーバ 106、清算装置 108 が配備されている。なお、門、ドア等の物理的な複数のゲートには、これらゲートを開閉制御するゲート制御部 101 が設けられている。

**【0010】**

また、複数のゲートには、RFIDタグ（非接触IC）104内の不揮発性メモリ201（図2参照）にアクセスするためのリーダ／ライタ109も設置されている。また、各ゲートに設置された各リーダ／ライタ109は、第1のネットワーク102によって相互に接続されており、この第1のネットワーク102には、ゲート制御部101、セキュリティサーバ103も接続されている。

#### 【0011】

このようなネットワーク構成の下で、RFIDタグ104内の不揮発性メモリ201に格納されたユーザID401（図4参照）をリーダ／ライタ109で読み出してセキュリティサーバ103に転送し、このセキュリティサーバ103にて当該ユーザの入退出入を管理すると共に、ゲート制御部101を介してゲートを開閉することにより、セキュリティエリア100を形成している。

#### 【0012】

なお、本実施形態では、セキュリティサーバ103によるユーザの入退出入管理に応じて、物理的なゲートをゲート制御部101により開閉制御しているが、必ずしも物理的なゲートをゲート制御部101により開閉制御する必要はない。

#### 【0013】

また、後で詳細に説明するように、機密データ（ジョブ情報、コマンドを含む）が格納されRFIDタグ104をセキュリティエリア100の外に持ち出す場合は、RFIDタグ104内の機密データをリーダ／ライタ109で読み出してセキュリティサーバ103に退避すると共に、RFIDタグ104内の機密データを消去することにより、セキュリティエリア100外で機密データが第三者に漏洩するのを防止している。

#### 【0014】

また、RFIDタグ104をセキュリティエリア100の中に再度持ち込む場合に、セキュリティサーバ103に退避した機密データをリーダ／ライタ109を介してRFIDタグ104に書き戻すことにより、セキュリティエリア100内で機密データを自由に利用できるようにしている。

#### 【0015】

セキュリティエリア100内のMFP（複合機）105、清算装置108には、それぞれ、リーダ／ライタ105a、108aが搭載されており、後述するように、セキュリティエリア100内では、MFP（複合機）105、清算装置108は、それぞれリーダ／ライタ105a、108aを介して、RFIDタグ104内のメモリに対して自由にアクセスできるように構成されている。

#### 【0016】

なお、第1のネットワーク102は、機密性を向上させるため、外界のネットワーク（インターネット等）とは物理的に分離されていることが望ましいが、物理的に分離することなく、ゲートウェイ等により情報的に分離するようにしてもよい。

#### 【0017】

MFP105と文書サーバ106は、第2のネットワーク107を介して接続されている。この第2のネットワーク107は、LAN、SAN（Storage Area Network）等により構成されているが、必ずしも第1のネットワーク102と物理的に接続されている必要はない。

#### 【0018】

MFP105に対するRFIDタグ104の利用形態としては、MFP105に搭載されたリーダ／ライタ105aにRFIDタグ104をかざすことで、このRFIDタグ104に格納されたFAX送信先情報、電子メールアドレス、文書サーバ106に格納された文書データの位置情報等を非接触にてMFP105にダウンロードし、それぞれFAX送信、電子メール送信、文書印刷出力を実行させること等が可能である。また、MFP105に搭載されたリーダ／ライタ105aにRFIDタグ104を近づけた状態で、MFP105の操作部（不図示）からFAX送信先情報、メールアドレス、文書サーバ106に格納された文書データの位置情報等を入力し、リーダ／ライタ105aを介して非接触

にてRFIDタグ104に格納することも可能である。

【0019】

清算装置108は、例えば食堂等に設置されており、この清算装置108に対するRFIDタグ104の利用形態としては、例えば清算装置108がRFIDタグ104に格納されたユーザID等に基づいて清算処理を行うことが可能である。この際、清算処理としては、予めプリペイドカード方式で入金を行っておくことで、RFIDタグ104に格納された残高情報を元に清算する方式でも、或いは清算装置108に接続された清算用サーバ（不図示）によって、ユーザ毎の代金情報を上記清算サーバ内に積算・記憶し、1ヶ月等の間隔で清算を行うような構成でもよい。また、毎回の食事の内容等を上記清算サーバ又はRFIDタグ104に格納し、後から履歴を参照できる構成にしてもよい。

【0020】

上記MFP105及び、清算装置108に対するRFIDタグ104の利用形態は、あくまでも一例であり、且つ本発明とは直接関係が無いため、詳細な説明は省略する。なお、RFIDタグ104は、上記MFP105、清算装置108以外のセキュリティエリア100内の各種の電子情報機器で利用することができる。

【0021】

[RFIDタグ]

図2は、RFIDタグ104の構成を示すブロック図である。RFIDタグ104は、非接触ICチップ、或いはデータキャリアとも呼ばれ、リーダ／ライタと無線で（すなわち非接触で）通信することが可能となっている。本実施形態では、カード型のRFIDタグを想定しており、このカード型RFIDタグ内には、以下のデバイスを内蔵した非接触ICチップが内包されている。

【0022】

すなわち、RFIDタグ（非接触ICチップ）104には、不揮発性メモリ201、電波を送受信するためのアンテナ部202、共振コンデンサ部203、電流の整流・平滑を行うための電力生成部204、電波の復調・変調を行うための復変調回路205、及び制御部206が形成されている。このRFIDタグ104は、バッテリー等の電源を内蔵しておらず、リーダ／ライタから供給される電波に基づいて電力を誘電している。

【0023】

すなわち、アンテナ部202は、共振コンデンサ部203との組み合わせで共振回路を形成している。一方、リーダ／ライタは、後述するように、常時、電力生成用の電波（交流磁界）を発している。このリーダ／ライタにRFIDタグ104をかざすと、RFIDタグ104内の上記共振回路には電磁誘導作用により誘導電流が発生する。この誘導電流は、電力生成部204に出力され、電力生成部204は、入力された誘導電流を整流・平滑して所定電圧の電力を生成し、不揮発性メモリ201、制御部206、復変調回路205に供給する。制御部206は、RFIDタグ104を全体的に制御するものである。

【0024】

リーダ／ライタは、電力生成用の電波信号の他に各種のデータに係る電波信号も同時に送信しており、このデータに係る電波信号は、復変調回路205によって復調され、制御部206の制御の下に不揮発性メモリ201に書き込まれる。また、制御部206は、不揮発性メモリ201からデータを読み出し、復変調回路205によって変調してアンテナ部202を介して電波信号として送信する。

【0025】

なお、制御部206は、ROM（図示省略）を内蔵しており、このROMには、図5のフローチャートにおけるステップS502、S505～S510、図6のフローチャートにおけるステップS602、S606に対応するアプリケーションプログラムが格納されている。ただし、このアプリケーションプログラムは、不揮発性メモリ201に格納してもよい。

【0026】

[リーダ／ライタ]

図3は、リーダ/ライタ109、105a、108aの構成を示すブロック図である。リーダ/ライタ109、105a、108aは、電波信号を送信するための送信アンテナ部301と、送信アンテナ部301から送信するデータ信号を変調する変調回路302と、電波信号を受信する受信アンテナ部303、受信アンテナ部303より受信した電波信号を復調する復調回路304、上位機器（本実施形態では、セキュリティサーバ103）との通信を行うI/F部306、及び制御部305を有しており、制御部305は、上記送信アンテナ部301、変調回路302、受信アンテナ部303、復調回路304、及びI/F部306を制御している。なお、送信アンテナ部301には、前述の電力生成用の電波を発するための交流電源307が接続されている。

#### 【0027】

制御部305は、セキュリティサーバ103からの指示により、変調回路302を用いて電力を供給するための電波、及び送信するデータを変調して、送信アンテナ部301を介して電波を発信させる。また、制御部305は、受信アンテナ部303で受信した電波信号を、復調回路304により復調させた後、データ信号として扱えるように変換することができる。

#### 【0028】

なお、制御部305は、ROM（図示省略）を内蔵しており、このROMには、図5のフローチャートにおけるステップS502、S505～S510、図6のフローチャートにおけるステップS602、S606に対応するアプリケーションプログラムが格納されている。

#### 【0029】

##### 〔RFIDタグの格納データ〕

図4は、RFIDタグ104の不揮発性メモリ201に格納されたデータを示す概念図である。

#### 【0030】

RFIDタグ104内の不揮発性メモリ201には、当該RFIDタグ104の所有者のユーザID401と個別データ402が格納されている。このユーザID401としては、各RFIDタグ104に対してそれぞれに固有の値（数値、記号等）が割り振られており、このユーザID401に基づいて当該RFIDタグ104を所有するユーザを認証することができる。すなわち、各RFIDタグ104内の不揮発性メモリ201に格納された各ユーザID401は、本システムの運用前に予めセキュリティサーバ103に登録されており、例えばゲートを通過する際に、リーダ/ライタ109によりRFIDタグ104からユーザID401を読み取り、セキュリティサーバ103に登録されたユーザID等と照合することで、当該ユーザがゲートを通過しても良いか否かを判断し（これを認証と呼ぶ）、入場/退出した旨がセキュリティサーバ103に記録される。

#### 【0031】

個別データ402は、1つのRFIDタグ104内に1つ又は複数の個別データ202が格納されている。各個別データ402は、それぞれ個別データID403、データ本体404、機密フラグ405によって構成されている。

#### 【0032】

個別データID403は、各個別データ402（すなわち、データ本体404）を識別するためのIDであり、電力生成用の電波信号個別データ402毎に固有の値（数値、記号等）が割り振られており、ユーザID401と組み合わせることで、MFP105や清算装置108に対して、データ本体404の各種データを授受することができる。

#### 【0033】

データ本体404は、実際に読み書きされて各種処理に用いられる個別データ402の実体をなすデータであり、前述のように、MFP105に関するデータとしては、FAX送信先情報、電子メールアドレス、文書サーバ106に格納された文書データの位置情報等が読み書きされ、なお、MFP105操作部から入力された情報を追加、或いは上書きすることも可能である。



## 【0034】

また、清算装置108に関するデータとしては、予め入金された金銭データや、食事の履歴情報が読み書きされる。なお、金銭データは清算装置108に接続された清算サーバ(不図示)によってのみ書き換えられる情報である。食事の履歴情報は、清算装置108によって書き換えられる情報である。

## 【0035】

機密フラグ405は、個別データ402毎に設定される情報であり、当該個別データ402が機密情報を含むのか否かを表している。本実施形態では、機密フラグ405がON(1)の場合は機密情報を含み、OFF(0)の場合は機密情報を含まないものと定義している。この機密フラグ405は、セキュリティサーバ103に接続されるリーダ/ライタ109でのみ書き込みが可能となっている。

## 【0036】

なお、本明細書では、機密フラグ405がONとなっている個別データ402については、その個別データ402の全部が機密事項ではなく一部だけが機密事項となっている場合も、当該個別データ402全体を機密データと呼んでいる(特許請求の範囲も同趣旨)。

## 【0037】

## [退出処理]

次に、セキュリティエリア100の中から外部に退出する場合の処理を、図5のフローチャートに基づいて説明する。

## 【0038】

ユーザが、セキュリティエリア100内から外部に退出する際に、ゲートに設置されたリーダ/ライタ109にRFIDタグ104をかざす(ステップS501)。すると、RFIDタグ104には、リーダ/ライタ109から発せられた電波により電力が誘電され、リーダ/ライタ109との通信が可能となる。そこで、リーダ/ライタ109の制御部305は、RFIDタグ104の制御部206と協働して、RFIDタグ104内の不揮発性メモリ201から、ユーザID401を読み出してセキュリティサーバ103に送信する。(ステップS502)。

## 【0039】

セキュリティサーバ103は、リーダ/ライタ109から受信したユーザID401が、当該セキュリティサーバ103に登録されており、かつ、そのユーザID401に係るユーザの入退出の状況が「入場」となっているか否かを判別することにより、当該ユーザの退出を認証するか否かを判別する(ステップS503)。

## 【0040】

セキュリティサーバ103は、受信に係るユーザID401が当該セキュリティサーバ103に登録されていない、或いは登録されていても当該ユーザID401に係るユーザの入退出の状況が「退出」となっている場合(この場合は、過去に不正にセキュリティエリア100内に入場したことを意味する)は、当該ユーザの退出を認証せずに、所定の警告処理を行って(ステップS504)、終了する。この警告処理としては、例えば、ゲートに設置された表示装置(図示省略)に警告メッセージを表示する、ゲートに設置されたスピーカ(図示省略)により警告音を鳴らす、或いはゲート制御部101によりゲートを一時的に閉鎖状態にロックさせること等が考えられる。

## 【0041】

一方、セキュリティサーバ103は、受信に係るユーザID401が当該セキュリティサーバ103に登録され、かつ当該ユーザID401に係るユーザの入退出の状況が「入場」となっている場合は、当該ユーザの退出を認証し、当該ユーザID401に係るユーザの入退出の状況を「退出」に変更し、当該ユーザの退出を認証した旨の情報をリーダ/ライタ109に通知する(ステップS505)。

## 【0042】

なお、本実施形態では、セキュリティサーバ103のメモリ容量を削減するため、セキ

セキュリティサーバ103は、最新の入退出状況だけを記憶しているが、過去の全て、或いは複数の入退出状況（履歴）を記憶するようにしてもよい。

#### 【0043】

リーダ／ライタ109の制御部305は、当該ユーザの退出を認証した旨の情報を受信すると、RFIDタグ104の制御部206と協働して、RFIDタグ104内の不揮発性メモリ201から、1つの個別データ402に係る個別データID403と機密フラグ405を読み出して（ステップS506）、機密フラグ405がONとなっているか否かを判別する（ステップS507）。

#### 【0044】

その結果、機密フラグ405がONとなっていれば、リーダ／ライタ109の制御部305は、RFIDタグ104の制御部206と協働して、対応する個別データ402（データ本体404）をRFIDタグ104内の不揮発性メモリ201から読み出して、セキュリティサーバ103に退避させ（ステップS508）、不揮発性メモリ201上の当該個別データ402を消去して（ステップS509）、ステップS510に進む。一方、機密フラグ405がOFFとなっていれば、リーダ／ライタ109の制御部305は、ステップS508の退避処理、ステップS509の消去処理を行うことなく、ステップS510に進む。

#### 【0045】

ステップS510では、リーダ／ライタ109の制御部305は、RFIDタグ104の制御部206と協働して、RFIDタグ104内の不揮発性メモリ201を参照し、機密フラグ405のチェック等を行っていない次の個別データ402が存在するか否かを判別する。その結果、機密フラグ405のチェック等を行っていない次の個別データ402が存在すれば、リーダ／ライタ109の制御部305は、ステップS506に戻り、当該次の個別データ402に対して同様の処理を行う。

#### 【0046】

一方、全ての個別データ402に対する機密フラグ405のチェック等の処理が完了した場合は、リーダ／ライタ109の制御部305は、例えばゲート制御部101によりゲートをオープンさせる等の入場処理を行い（ステップS511）、本処理を終了する。

#### 【0047】

##### 〔入場処理〕

次に、セキュリティエリア100の中から外部に退出する場合の処理を、図5のフローチャートに基づいて説明する。

#### 【0048】

ユーザは、セキュリティエリア100の外から内部に入場する際に、ゲートに設置されたリーダ／ライタ109にRFIDタグ104をかざす（ステップS601）。すると、RFIDタグ104には、リーダ／ライタ109から発せられた電波により電力が誘電され、リーダ／ライタ109との通信が可能となる。そこで、リーダ／ライタ109の制御部305は、RFIDタグ104の制御部206と協働して、RFIDタグ104内の不揮発性メモリ201から、ユーザID401を読み出してセキュリティサーバ103に送信する。（ステップS602）。

#### 【0049】

セキュリティサーバ103は、リーダ／ライタ109から受信したユーザID401が、当該セキュリティサーバ103に登録されており、かつ、そのユーザID401に係るユーザの入退出の状況が「退出」となっているか否かを判別することにより、当該ユーザの入場を認証するか否かを判別する（ステップS603）。

#### 【0050】

セキュリティサーバ103は、受信に係るユーザID401が当該セキュリティサーバ103に登録されていない、或いは登録されていても当該ユーザID401に係るユーザの入退出の状況が「入場」となっている場合（この場合は、過去に不正にセキュリティエリア100の外に退出したことを意味する）は、当該ユーザの入場を認証せずに、所定の

警告処理を行って（ステップS604）、終了する。この警告処理としては、例えば、ゲートに設置された表示装置に警告メッセージを表示する、ゲートに設置されたスピーカにより警告音を鳴らす、或いはゲート制御部101によりゲートを一時的に閉鎖状態にロックさせること等が考えられる。

#### 【0051】

一方、セキュリティサーバ103は、受信に係るユーザID401が当該セキュリティサーバ103に登録され、かつ当該ユーザID401に係るユーザの入退出の状況が「退出」となっている場合は、当該ユーザの入場を認証し、当該ユーザID401に係るユーザの入退出の状況を「入場」に変更し、当該ユーザの入場を認証した旨の情報をリーダー/ライター109に通知する（ステップS605）。

#### 【0052】

リーダー/ライター109の制御部305は、当該ユーザID401に係るユーザの入場を認証した旨の情報を受信すると、当該ユーザID401に係る退避された個別データ402をセキュリティサーバ103に照会して送信してもらい、RFIDタグ104の制御部206と協働して、RFIDタグ104内の不揮発性メモリ201に書き戻す（ステップS606）。

#### 【0053】

次に、リーダー/ライター109の制御部305は、当該ユーザID401に係る退避された他の個別データ402が存在するか否かをセキュリティサーバ103に問合せ（ステップS607）、退避された他の個別データ402が存在する場合は、ステップS606に戻ることに伴い、当該他の個別データ402をRFIDタグ104内の不揮発性メモリ201に書き戻す。

#### 【0054】

なお、セキュリティサーバ103は、セキュリティサーバ103内のメモリ（図示省略）を有効利用するため、書き戻した個別データ402は消去している。また、セキュリティサーバ103は、上記のように、リーダー/ライター109の制御部305からの照会や問合せに回答して、退避に係る個別データ402をリーダー/ライター109に送信するのではなく、ステップS602でリーダー/ライター109から受信したユーザID401に基づいて、能動的に退避に係る個別データ402を検索してリーダー/ライター109に送信するようにしてもよい。

#### 【0055】

一方、退避された他の個別データ402が存在しない場合は、リーダー/ライター109の制御部305は、例えばゲート制御部101によりゲートをオープンさせる等の入場処理を行い（ステップS608）、本処理を終了する。

#### 【0056】

このように、本実施形態では、セキュリティエリア100の外にRFIDタグ104を持ち出す場合に、RFIDタグ104から機密データを読み出してセキュリティサーバ103に退避した後に、RFIDタグ104上の退避に係る機密データを消去し、セキュリティエリア100の中にRFIDタグ104を持ち込む場合に、退避に係る機密データをRFIDタグ104に書き戻して復元しているので、機密データがセキュリティエリア100の外で第三者に漏れて悪用されるのを回避することが可能となる。また、機密データの退避、消去、書き戻し処理は、RFIDタグ104をリーダー/ライター109にかざした際に自動的に行われるので、ユーザの負担が増大することはない。

#### 【0057】

また、RFIDタグ104にはバッテリーを搭載する必要がないので、RFIDタグ104の小型化が可能になると共に、セキュリティシステムを安価に構築することが可能となる。さらに、ユーザ認証を受けないと機密データの復元は行われないので、万一、ユーザ認証を受けずに不正にセキュリティエリア100の中に入場したとしても、機密データを利用できなくなり、セキュリティ機能が更に向上する。

#### 【0058】

**【実施形態の変形例】**

上記のように、RFIDタグ104に格納された機密データを退避、消去、書戻しを行うことなく、以下のようにして、機密データの漏洩を防止するようにしてもよい。

**【0059】**

すなわち、個別データ402の構成データとして、読出可能フラグを定義し、セキュリティエリア100の外にRFIDタグ104を持出す際には、機密データに係る読出可能フラグを読出不可状態に設定し、且つセキュリティエリア100の中にRFIDタグ104を持ち込む際には、機密データに係る読出可能フラグを読出可能状態に設定することで、セキュリティエリア100の外では、機密データの漏洩を防止すると共に、セキュリティエリア100の中では、機密データを自由に利用できるようにしてもよい。

**【0060】**

この場合、上記読出可能フラグは、上記セキュリティサーバ103によって当該RFIDタグ104のユーザが認証された場合にのみ、例えばリーダー/ライター109によりフラグ値を変更できるようにする必要がある。また、RFIDタグ104においては、制御部206、又はメモリコントローラ（不図示）内に、上記読出可能フラグが読出不可状態に設定された個別データ（機密データ）を読出せないようにする制御機構を設け、RFIDタグ用の市販のリーダー/ライター等では、この機密データを読出せないようにする必要がある。

**【0061】**

なお、上記実施形態例では、機密データの退避、消去、或いは書戻しの処理を行う必要があるため、入退出管理に要する時間が長くなる可能性が考えられる。一方、変形例では、機密データを直接処理することはないので、入退出管理に要する時間は短くなるが、機密データが形式上セキュリティエリア100の外に持ち出されてしまい、セキュリティの点では多少の不安が残る。上記実施形態例と変形例の何れを選択するかは、セキュリティ性と入退出管理の所要時間との何れを重要視するかで決定すればよい。

**【0062】**

なお、個別データ402の構成データとして、上記読出可能フラグの代わりに、アクセス可能フラグを定義することにより、機密データの上に他のデータが書き込まれる等して機密データが破壊されるのを防止することも可能である。

**【0063】**

また、上記のようにRFIDタグを入退出管理に利用せず、各種の装置で使用するデータを記録するだけの目的で利用する場合にも、本発明を適用することが可能である。この場合は、機密エリアに対するRFIDタグの持出し/持込みを検知する手段としては、RFIDタグ用のリーダー/ライターを用いる必要はなく、例えば、パチンコ店、ゲームセンター等の遊技場でRFIDタグを遊戯代金の清算媒体として利用するような場合において、所定の装置により遊技場に磁場（すなわち、機密エリア）を形成し、RFIDタグには磁場を検知するデバイスを搭載し、このデバイスにより機密エリアに対するRFIDタグの持出し/持込みを検知することも可能である。

**【0064】**

なお、上記の遊技場でRFIDタグを遊戯代金の清算媒体として利用する例では、上記実施形態、又は変形例に係る機密データの漏洩防止処理は、RFIDタグに格納されたプレイカード情報が他の経営者に係る遊技場で使用されるのを回避するために行われる。

**【0065】**

また、RFIDタグにバッテリーを搭載することも可能である。この場合は、RFIDタグの制御部は、リーダー/ライターの制御部と協働することなく、主体的に上記実施形態、又は変形例に係る機密データの漏洩防止処理を実行するように構成することも可能である。

**【0066】**

さらに、機密データの漏洩防止処理として、機密エリアの外にRFIDタグを持出す際に、当該RFIDタグ内の機密データを暗号化し、機密エリアの中にRFIDタグを持ち込む際に（必要に応じてユーザ認証も行って）、当該RFIDタグ内の暗号化された機密デ

ータを復号化することも可能である。

【0067】

また、RFIDタグの通信方式は、電波、又は電磁波を用いることなく、例えば、赤外線等の光を用いた通信方式でもよい。また、RFIDタグの形状は、カード型でなく、ラベル型、コイン型、箱型、スティック型等であってもよい。

【0068】

さらに、本発明の目的は、上記実施形態、変形例等の機能を実現するソフトウェアのプログラムコードをRFIDタグ、リーダ／ライタに無線通信等により非接触でダウンロードし、RFIDタグ、リーダ／ライタの制御部がダウンロードに係るプログラムコードを実行することによっても、達成されることは言うまでもない。

【0069】

この場合、上記プログラムコード自体が前述した実施形態、変形例等の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、上記プログラムコードを実行することにより、前述した実施形態、変形例等の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、RFIDタグ、リーダ／ライタ上で稼動しているオペレーティングシステム（OS）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態、変形例等の機能が実現される場合も含まれることは言うまでもない。

【図面の簡単な説明】

【0070】

【図1】本発明を実施するための最良の形態に係るセキュリティシステムの概略構成を示すシステム構成図である。

【図2】上記セキュリティシステムのRFIDタグの概略構成を示すブロック図である。

【図3】上記セキュリティシステムのリーダ／ライタの概略構成を示すブロック図である。

【図4】上記RFIDタグの不揮発性メモリ内のデータの構成を示す概念図である。

【図5】セキュリティエリアからRFIDタグを持ち出す場合のセキュリティシステムの処理を示すフローチャートである。

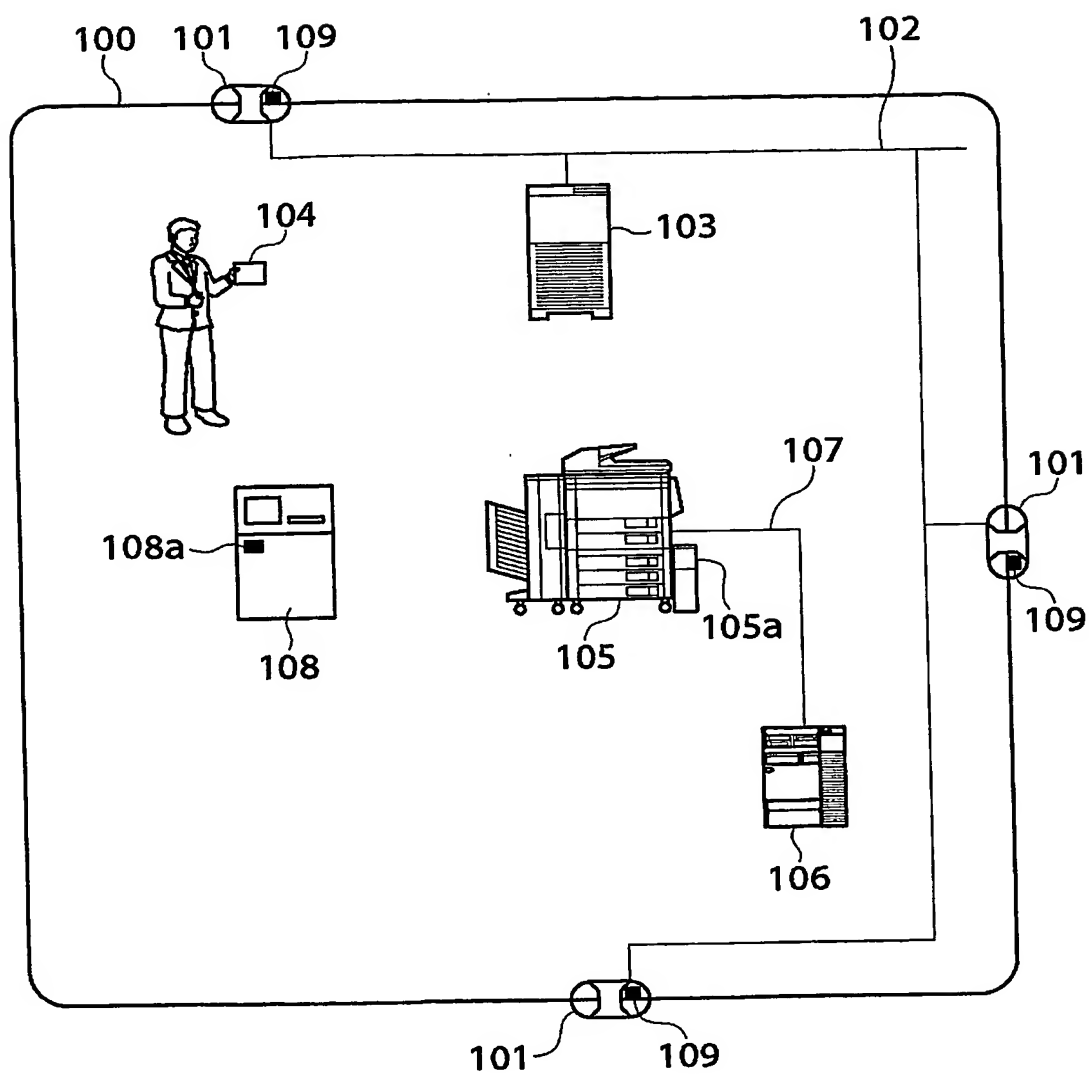
【図6】セキュリティエリアにRFIDタグを持ち込む場合のセキュリティシステムの処理を示すフローチャートである。

【符号の説明】

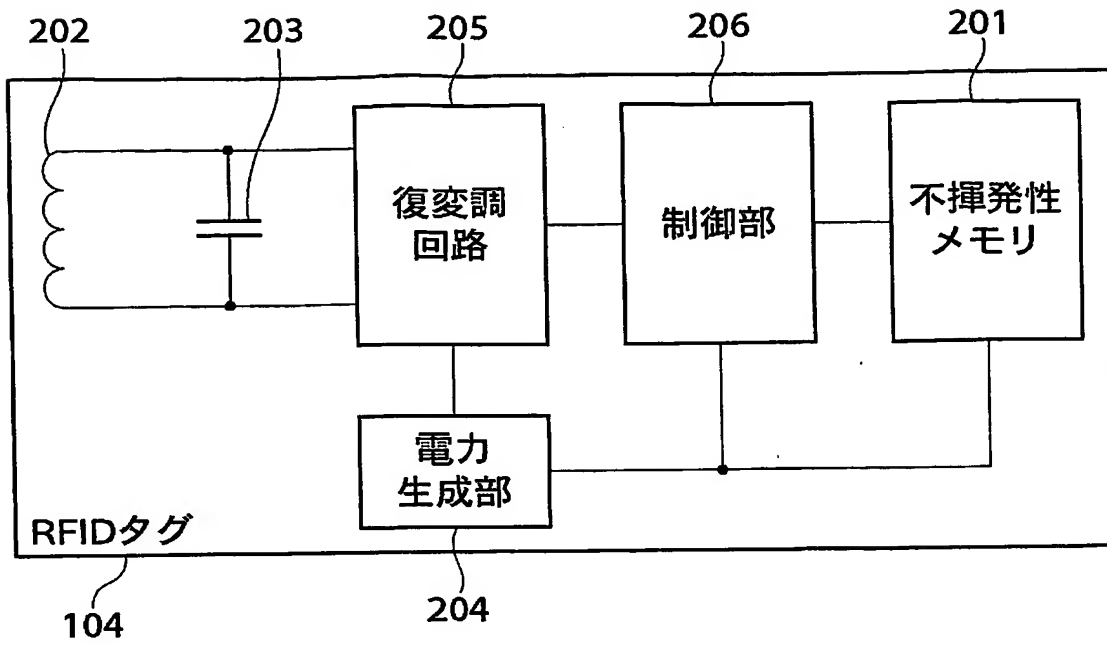
【0071】

- 100…セキュリティエリア
- 101…ゲート制御部
- 103…セキュリティサーバ
- 104…RFIDタグ
- 109、105a、108a…リーダ／ライタ
- 201…不揮発性メモリ
- 205…RFIDタグの制御部
- 305…リーダ／ライタの制御部
- 401…ユーザID
- 402…個別データ
- 405…機密フラグ

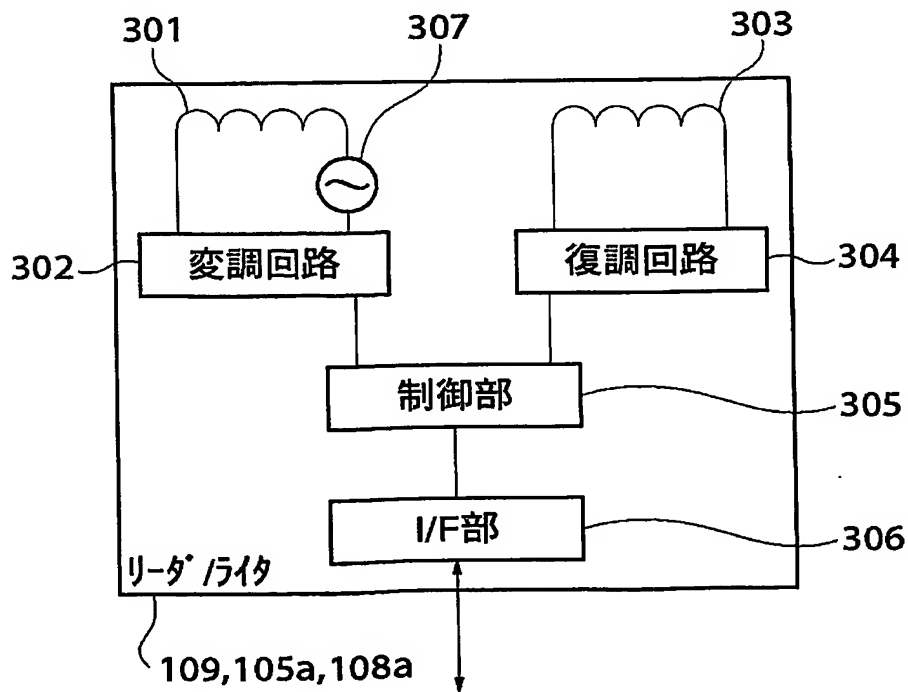
【書類名】 図面  
【図 1】



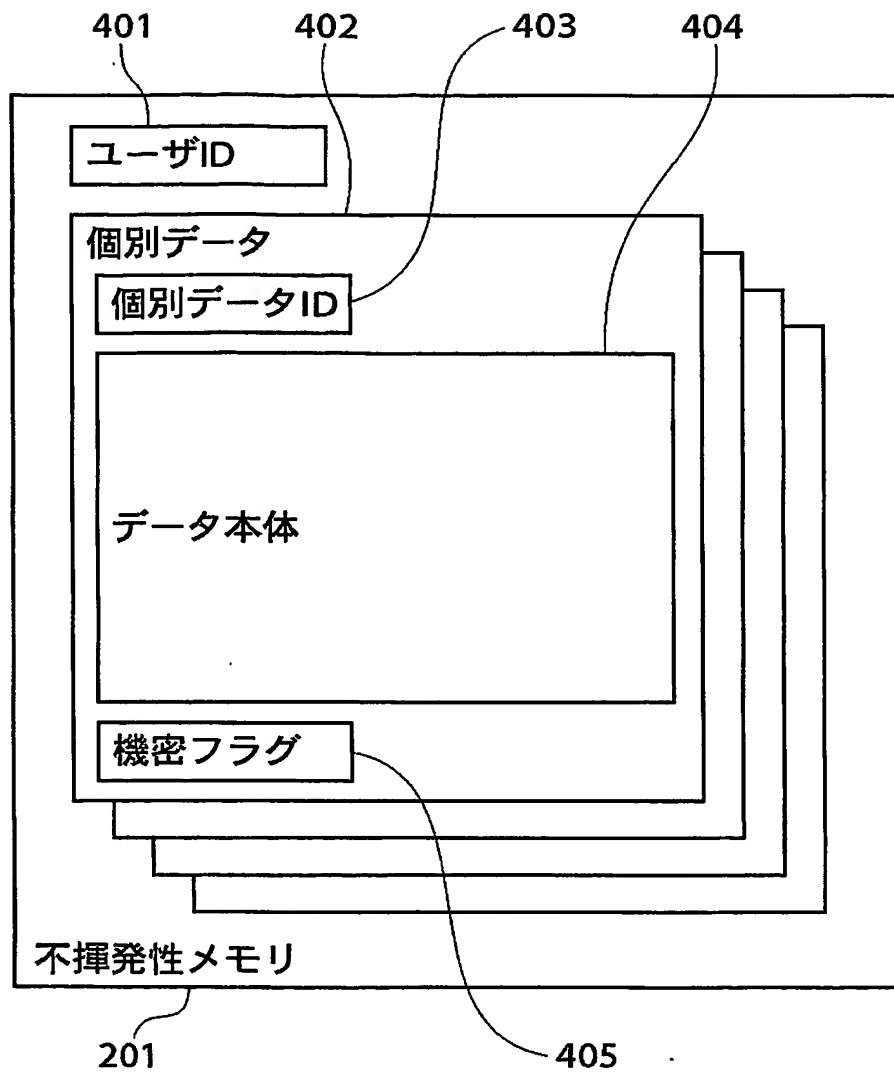
【図 2】



【図 3】

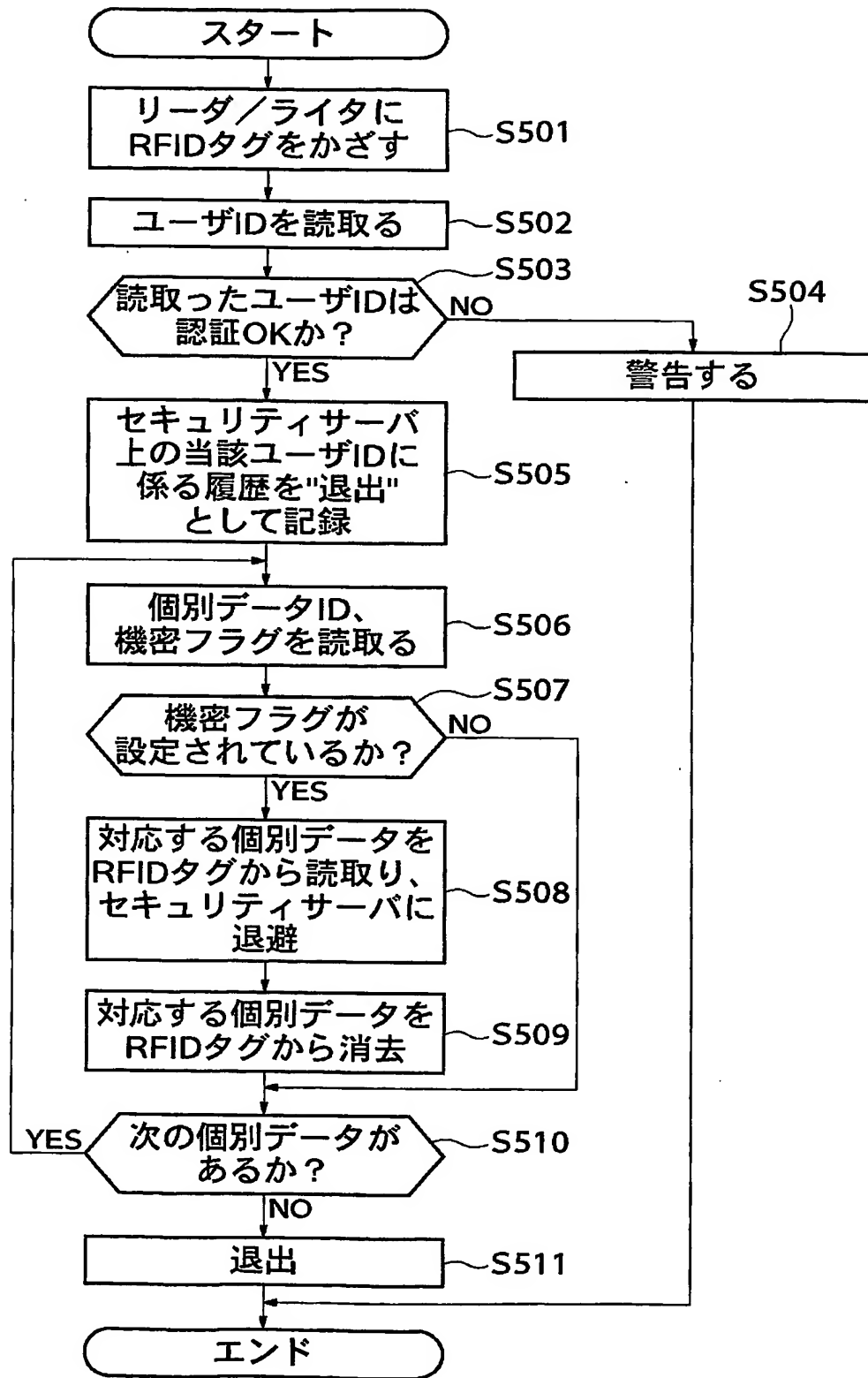


【図 4】

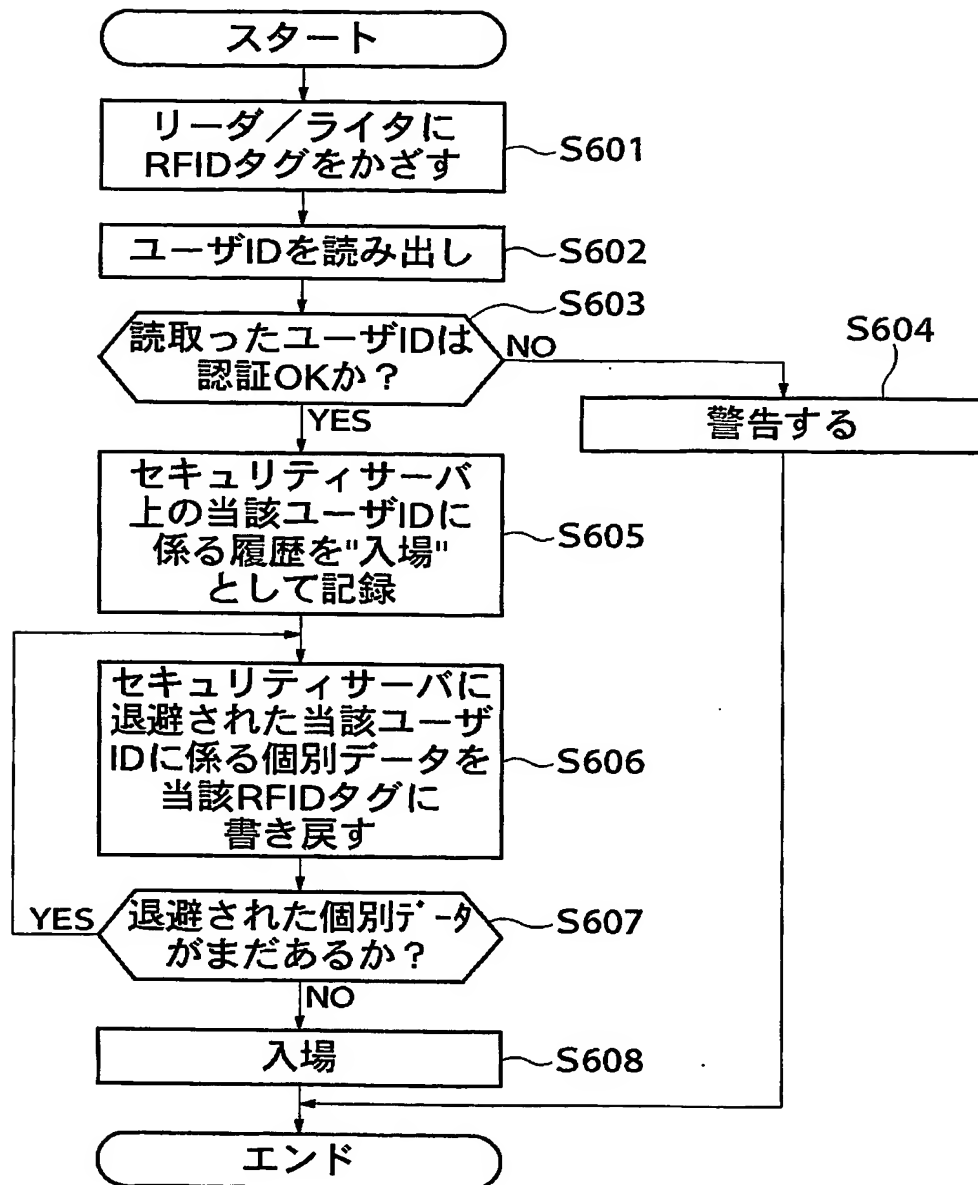




【図 5】



【図 6】



## 【書類名】要約書

## 【要約】

【課題】 非接触 IC に格納された機密データが所定エリア外で第 3 者に漏洩するのを防止できるようにする。

【解決手段】 セキュリティエリア 100 の外に RFID タグ 104 を持ち出す場合に、RFID タグ 104 から機密データを読み出してセキュリティサーバ 103 に退避した後に、RFID タグ 104 から退避に係る機密データを消去し、セキュリティエリア 100 の中に RFID タグ 104 を持ち込む場合に、RFID タグ 104 に退避に係る機密データを書き戻して復元する。

【選択図】 図 1

特願 2 0 0 3 - 3 9 2 3 7 7

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 1 0 0 7 ]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都大田区下丸子3丁目30番2号

氏 名

キヤノン株式会社

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**